WILLKIE FARR & GALLAGHER LLP
BENEDICT HUR (SBN 224018)
bhur@willkie.com
SIMONA AGNOLUCCI (SBN 246943)
sagnolucci@willkie.com
EDUARDO SANTACANA (SBN 281668)
esantacana@willkie.com
JOSHUA D. ANDERSON (SBN 312836)
jdanderson@willkie.com
DAVID D. DOAK (SBN 301319)
ddoak@willkie.com
TIFFANY LIN (SBN 321472)
tlin@willkie.com
HARRIS MATEEN (SBN 335593)
hmateen@willkie.com
NAIARA TOKER (SBN 346145)
ntoker@willkie.com
NADIM HOUSSAIN (SBN 335556)
nhoussain@willkie.com
333 Bush Street, 34th Floor
San Francisco, California 94104
Telephone: (415) 858-7400

Attorneys for Defendant
GOOGLE LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JOHN DOE I, et al., individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

GOOGLE LLC,

Defendant.

Case No. 3:23-cv-02431-VC
(Consol. w/ 3:32-cv-02343-VC)

DEFENDANT GOOGLE LLC'S REPLY IN SUPPORT OF ITS MOTION TO DISMISS SECOND AMENDED COMPLAINT

Date: November 7, 2024
Time: 10:00 a.m.
Ctrm.: 4 – 17th Floor, San Francisco
Before: Hon. Vince Chhabria

Consol. Complaint Filed: July 13, 2023
2nd Am. Complaint Filed: August 12, 2024

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

I. INTRODUCTION

The Opposition continues to ignore the fundamental problems in Plaintiffs' sixth complaint. It asks the Court to believe that healthcare providers and Google conspired to breach Google's contractual terms and federal healthcare privacy law so Google could take possession of health data it says it does not want and should not receive, in order to target advertising based on characteristics it says it will not use, so that it may make more money on advertising (the healthcare providers' incentive to cooperate in this alleged conspiracy is unclear). And, Plaintiffs argue, this is clear from none other than Google's public commitment not to do any of this. Apart from that, Plaintiffs allege *nothing* to support their theory of the case: not one advertisement targeted based on a health characteristic to any person, ever; no report or study or analysis that any such targeting has ever happened; no individual who experienced a single harm; no acknowledgment by any participant of this alleged conspiracy that it existed and was effectuated; not even a competent allegation that Google's technology was incorporated on any specific webpage in any particular manner that would result in the transmission of any specific health data.

Here is what really happened here. This case was filed on a guess, and the guess turned out to be wrong. As Google proved at the preliminary injunction stage, it took affirmative steps (that it was never required to take) to *ensure* that even if the specific healthcare providers at issue breached Google's terms, Google's ads infrastructure would *still* not use the data in an offending way. Not content to walk away from their bad guess, Plaintiffs have turned their focus from advertising, alleging now that Google puts health data to use in other nonsensical ways and relitigating the Court's last decision. But, at bottom, the new complaint is just as flawed as the last five. The case should be dismissed with prejudice.

II. ARGUMENT

A. This Court should apply Rule 9(b).

By necessity, Plaintiffs' theory of the case hinges on allegations of fraud, requiring Plaintiffs to satisfy the heightened pleading requirements of Rule 9(b). Their theory of the case could not proceed any other way, because Google publicly denies the wrongdoing alleged, forbids

it from its commercial partners, and discusses steps it takes to protect the public from the alleged injuries; and, as Plaintiffs know from the preliminary injunction ("PI"), Google did, in fact, classify the Websites raised in the PI motion as sensitive or mixed content, disabling any use of their data in the allegedly injurious manner. *See* Dkt. 48-24. So, for Plaintiffs, it must be fraud, and fraud is the theory they press to this Court once again, subjecting them to Rule 9(b)'s heightened pleading standard. *See Rodriguez v. Google LLC*, 2021 WL 2026726, at *3 (N.D. Cal. May 21, 2021).

Plaintiffs argue that, under *Smith v. Google*, 2024 WL 2808270, at *5 (N.D. Cal. June 3, 2024), a single example of a district court refusing to apply Rule 9(b) in this way, they can allege intent generally and move on. Dkt. 169 ("Opp.") at 11. They are doubly mistaken. Intent is not the only element of fraud they allege; they also allege a uniform course of fraudulent conduct to deceive the public about the true functioning of Google technology. And regardless, it is the Ninth Circuit that binds, and its position on this is clear: Rule 9(b) is not reserved solely for claims of fraud, but material allegations of fraud, too. As Judge Fletcher put it in terms irreconcilable with the reasoning in *Smith* (which failed to cite binding precedent): "In cases where fraud is not a necessary element of a claim . . . . the plaintiff may allege a unified course of fraudulent conduct and rely entirely on that course of conduct as the basis of a claim. In that event, the claim is said to be 'grounded in fraud' or to 'sound in fraud,' and the pleading of that claim as a whole must satisfy the particularity requirement of Rule 9(b)." *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003).

Plaintiffs do not deny that their claims rest on the notion that Google "conspired with Health Care Providers," "disguised" first-party "ghost cookies" as "third-party cookies," and created a "self-serving" and "farcical" HIPAA policy in order to defraud the public and make more profits. SAC ¶¶ 97–98, 153, 162, 256, 265–70. Indeed, the SAC claims that Google's terms and policies were purposefully misleading. SAC ¶¶ 155, 158–59. And the Opposition doubles down on this theory. *See* Opp. at 10 (alleging that Google's HIPAA policy was "*intended* to do no more than provide a modicum of deniability for Google"), 11–12 (claiming that Google "procured [websites' consent] by false pretenses, omission, or known mistake"), 13 (alleging that healthcare

providers worked *with* Google to violate the Federal Wiretap Act). Under *Vess*, a plaintiff cannot plead around Rule 9(b) while still taking advantage of the *in terrorem* effects of alleging fraudulent conduct. Rule 9(b) was made for cases like this.

And of course, Plaintiffs allege no facts to support their fraud allegations. Their perfunctory attempt to show that the SAC satisfies Rule 9(b) fails to cite any part of the SAC or provide the requisite "who, what, when, where, and how" of the alleged fraud. Opp. at 11. They state that Google marketed its products to healthcare providers by "downplaying and obscuring the truth" in unspecified "policy documents" "throughout the time each version of each document was posted." *Id.* This falls far short of the specificity required. As *Vess* explained, plaintiffs must "set forth more than the neutral facts necessary to identify the transaction. The plaintiff must set forth what is false or misleading about a statement, and why it is false." *Vess*, 317 F.3d at 1106.

B. Plaintiffs concede key factual elements of their claims.

1. Plaintiffs concede they never received offending ads.

Even when pointedly invited to by this Court and Google, Plaintiffs still fail to claim they saw any targeted ads or personalized content based on their interactions with the Websites. *See* Dkt. 164 ("Mot.") at 10–11. The conclusion is inescapable. And to distract from it, Plaintiffs now downplay "personalized advertising" as a "narrow subset" of the allegedly offending uses of the data at issue, claiming that "none of Plaintiffs' claims are based on receiving advertisements." Opp. at 7, 19. But Plaintiffs do not identify allegations to support *any* advertising-related allegations, personalized or otherwise. *See id.* Nor do Plaintiffs allege any instance of failure by Google to enforce its prohibitions, arguing only that Google's failure is that "Plaintiffs' Health Care Providers use Google Ads code on their web properties," *id.* at 7–8, even though all admit such a use can be lawful. And even such an instance would prove nothing, as it would not necessarily mean any of these Plaintiffs were harmed, nor that Google intended such an error to occur, nor that Google should be liable for a third party's alleged breach of its commercial terms. At this stage, it is not even clear Plaintiffs can support Article III standing, as it does not appear they themselves have ever experienced an ounce of injury of any kind.

2. Plaintiffs fail to identify transmitted Health Information.

Plaintiffs allege generally that the information Google collected was "sensitive" and "identifiable." Opp. at 2–4. But the SAC fails to include specific allegations regarding the allegedly problematic locations where the healthcare providers placed Google source code, and whether Plaintiffs themselves visited those locations; that is, was there code on pages that could have contained sensitive, identifiable information in the first place? Mot. at 7–8. The SAC relies heavily on "example transmissions" to explain where Plaintiffs believe the code was placed, but falls short of alleging that those transmissions pertain to Plaintiffs. And though the SAC lists certain URLs that Plaintiffs claim contained source code—*see* SAC ¶¶ 40, 48, 57, 62, 70, 76—Plaintiffs do not claim that they actually visited those URLs, and do not specify whether they are authenticated or unauthenticated pages. Mot. at 8–9. Plaintiffs do generally allege that they logged in to patient portals, but they stop short of alleging that any of the listed URLs they identify are listed are located within a patient portal (nor does it appear to be the case based on the URLs themselves, which appear to be available to any member of the public).

As a backdoor attempt to meet their burden, Plaintiffs cite a brief in *Doe I v. Medstar Health, Inc.*, No. 1:2023-cv-01198 (D. Md. May 5, 2023) to claim that Cerner "acknowledg[ed] it used Google Analytics 'to monitor user activity across its clients' [patient] portal domains,'" and that in turn two of the Websites used Cerner. Opp. at 2. A brief cannot substitute for factual allegations; in any event, *Doe I* was stayed pending the outcome of a state court proceeding in which the court ***dismissed plaintiffs' claims against MedStar on summary judgment***. Mot. at 4. If Plaintiffs' counsel insist on importing the records from their other cases, they should not be permitted to import them selectively. And needless to say, if they can't make a case against MedStar, they can't make one against Google for MedStar's conduct.

Likewise, Plaintiffs attach as Exhibit 4 to the SAC an unauthenticated meeting invite with someone at HHS that discusses research by a University of Illinois researcher that supposedly shows that Epic sent Google *the URLs and titles* of webpages users visited inside of MyChart portals, including at the Edward-Elmhurst Health website (and nothing more). Dkt. 158-4. By

contrast, the researcher claimed that Facebook received far more information from the same webpages: "personal information, such as name, address, phone number, email, gender, and birthday; medications; plans of care, including upcoming lab tests; information about appointments, including dates, hospitals, and topics." *Id.* at 1. In any case, as with Cerner, this is far short of the requisite showing, and the title of a webpage like "Health Record: Blood Pressure" is not in any reasonable sense "Health Information" as defined by the SAC. *See* SAC ¶ 21a. The only "inference about a consumer's health" one could draw from the sole webpage title on which Plaintiffs rely (which itself is not said to have related to Edward-Elmhurst anyway) is that someone—like everyone else—has blood pressure.

3. Plaintiffs fail to identify other sensitive or identifiable information.

Leaving behind their own definition of Health Information, Plaintiffs claim that Google "intercepted information showing when patients (including Plaintiffs) logged in to their patient portals" and when "patients use a provider's bill payment webpage." Opp. at 3. But the "example" transmissions they cite pertain to webpages that Plaintiffs did not visit. *Id.*; Mot. at 8–9. Moreover, Plaintiffs acknowledge that a login or bill payment webpage accessible to the public is not itself an authenticated webpage. *See* Mot. at 8 (noting that "user-authenticated webpages" are webpages that "require a user to log in before they are able to access the webpage"). And, as HHS has acknowledged, the use of tracking technology on healthcare provider webpages does not constitute individually identifiable health information "if the visit to the webpage is not related to an individual's past, present, or future health, health care, or payment for health care." *Id.*

Plaintiffs also claim that the information Google collected was "identifiable" because it contained cookies and IP addresses. Opp. at 3–4. However, they do not cite any authority under HHS, HIPAA, or elsewhere, supporting their contention that a pseudonymous cookie value (which is a string of randomized numbers, like 168457285.1684349681, *see* SAC ¶ 89), can reasonably be used to identify an individual, as opposed to, for example, a name, birth date, or social security number.[1] And, as discussed, websites had the option to truncate IP addresses in Universal

[1] Plaintiffs also contend that the data includes a "gtm" value, but that value identifies a website's Google Tag Manager account, not a person. Opp. at 4.

Analytics (the prior version of Google Analytics), and the current version of Google Analytics does not log or store IP addresses at all. Mot. at 16; Dkts. 165-7 and 165-8. In any event, having failed to allege receipt of Health Information, Google's alleged receipt of "cookies" or "IP addresses" cannot save their claims. That an anodyne data transmission is accompanied by an IP address is not unlawful; it is, in fact, exactly what HHS has acknowledged is routine for the lawful and appropriate use of analytics technology.

4. Plaintiffs concede their case does not encompass tangential products.

Plaintiffs' SAC "lacks any allegations relating to 'apps,' Google Tag, or Google Tag Manager." Mot. at 10. Plaintiffs do not dispute this, appearing to concede it.

C. Plaintiffs' allegations still fail to establish intent.

This Court ruled that awareness and intent are not the same thing, and that Plaintiffs failed to allege that Google acted "consciously and deliberately," fatally undermining each of Plaintiffs' claims, because Google forbade the Websites from sending HIPAA-covered information to Google, and Plaintiffs failed adequately to allege this prohibition was "just a ruse to mask the company's true objective." Dkt. 157 ("Order") at 9. The SAC adds nothing to this. Instead, Plaintiffs' *blockbuster* evidence of intent is the unsurprising and uninteresting fact that Google wanted healthcare providers (among those in many other industries) to use Google Analytics, which, as all acknowledge, is lawful. The "recently unsealed" 8-page excerpt of a 325-page 2017 strategy document notes only that the paid version of Google Analytics was "[t]argeted to Google's largest media-sales verticals (like Retail, Travel, Finance, and Technology) . . . with secondary focus on Classifieds and Local, Automotive, Healthcare, Education, and Media & Entertainment," and that Google's "objective is to grow coverage of the overall media measurement of these customers, and secondarily to drive new direct revenue for Google." Ex. 158-11 at 3. Nowhere in the document does Google state that it marketed Google Analytics in hopes of receiving and using health data, nor that it ever did receive it.

Secondarily, Plaintiffs claim that Google should have warned healthcare providers more strenuously than it did, and that because Google fell below Plaintiffs' self-defined standard for

HIPAA-related warnings, Google must have intended for healthcare providers to send it Health Information. Opp. at 6 n.1; *see also* SAC ¶ 152; Dkt. 165-5 at 4. Plaintiffs, however, are not responsible for setting the bar here and cite no authority for their position.

The Terms of Service, 2018 HIPAA policy, the updated 2023 HIPAA policy, and the Privacy Policy have always been clear that Google doesn't want to receive health information, that it doesn't intend to use it, and that healthcare providers shouldn't send any. And while the Court is not required to believe Google that it was telling the truth, Plaintiffs need to present something more than "Google should have warned more forcefully" for the Court to conclude, taking the allegations as true, that Google's secret intent was for its policies to be ignored.

In addition, the fact that some healthcare providers issued data breach notifications does not mean that Google's policies were insufficient, or that they were even violated; indeed, the data breach notifications that Plaintiffs attach do not mention Google's policies nor claim that Google's disclosures misled the providers. Mot. at 16. Nor do they specify that a single iota of information was actually improperly disclosed, much less used by Google for any purpose.

Finally, Plaintiffs claim that Google used and benefited from health information, so it must have intended to receive it. Opp. at 7. But there are no competent allegations that Google did use or benefit from health information—not for targeted advertising, personalized advertising, or any other purpose. *Infra* Section II.B.1; Mot. at 10–12. And even if healthcare providers had inadvertently transmitted health information to Google, that would have been against the clear prohibitions in Google's terms and policies, which negates any allegation of intent. If Google's ads machine accidentally swallowed contraband information alongside lawful information, and if it accidentally then used it for some purpose (which is not something Plaintiffs have competently alleged occurred even once), that still does not rise to the level of conscious and deliberate action; it doesn't even rise to the standard of mere "awareness" that Plaintiffs pressed in their opposition to the motion to dismiss.

D. Each of Plaintiffs' claims should be dismissed with prejudice.

1. Plaintiffs fail to state a Federal Wiretap Act claim (Count 1).

Plaintiffs seek a reconsideration of this Court's decision that the intent standard for a Federal Wiretap Act claim requires conscious and deliberate action, as the Ninth Circuit held in *United States v. Christensen*, 828 F.3d 763, 790–91 (9th Cir. 2015). *See* Order at 10; Opp. at 9. Plaintiffs argue that the intent element requires only that Google intend that the Websites use its technology. Opp. at 9. Plaintiffs' position is inconsistent with *Christensen* and the authority on which *Christensen* relies. *See Christensen*, 828 F.3d at 791; *In re Pharmatrak, Inc.*, 329 F.3d 9, 23 (1st Cir. 2003); *United States v. Townsend*, 987 F.2d 927, 931 (2d Cir. 1993) (finding intent where "Townsend intentionally intercepted communications between two unknowing and unconsenting individuals."). It also doesn't make any sense: all admit that there are lawful uses of Google's technology by the Websites, so intending that they use the technology cannot be unlawful. *See* Mot. at 22 (discussing HHS). As the First Circuit has previously held, "inadvertent interceptions are not a basis for criminal or civil liability under the ECPA." *In re Pharmatrak, Inc.*, 329 F.3d at 23. Taken on its face, Plaintiffs' position would bring about the absurd result that all source code providers would be liable under a criminal statute depending solely on whether the third party implementers of the source code use it lawfully or unlawfully.

On the question of consent, Plaintiffs add nothing to the prior dismissal, arguing again that the Websites did not consent to the transmission of PHI to Google. Opp. at 10–11. But as Plaintiffs' SAC acknowledges, the Websites determine whether to use, and on which pages to place Google's source code, as well as what data to transmit to Google using that source code. *See* SAC ¶¶ 86–87, 114, 154.

Finally, the crime-tort exception cannot invalidate the Websites' consent. *See* Opp. at 11–13; *Rodriguez*, 2021 WL 2026726, at *6 n.8. Despite the ink they spill on this subject, Plaintiffs add nothing new to this argument, either. *See* Mot. at 16–17.

2. Plaintiffs fail to state a CIPA claim (Count 2).

Plaintiffs still cannot allege that Google acted willfully to read the contents of Plaintiffs'

health information or intentionally recorded confidential communications, as required under CIPA Sections 631 and 632, respectively. Plaintiffs claim, without any authority, that the "willfulness" and "intent" requirements are satisfied simply because "Google read and learned the contents of their communications *by design*." Opp. at 14 (emphasis added). However, willfulness and intent require more than merely designing technology that developers can use to analyze *their own* website visitors' activity. *See, e.g.*, *Lozano v. City of Los Angeles*, 73 Cal. App. 5th 711, 728 (2022) (finding no intent where the allegations showed only that the defendant "understood it was deploying recording devices that *might* happen to record a confidential communication—not that [defendant] intended to record those communications."); *Rojas v. HSBC Card Servs. Inc.*, 20 Cal. App. 5th 427, 434 (2018) (citing *People v. Superior Court of Los Angeles County*, 70 Cal. 2d 123, 133 (1969) (rejecting plaintiff's argument that "the mere intent to activate a tape recorder which subsequently 'by chance' records a confidential communication is sufficient to constitute an offense under [Section 632] . . . . a necessary element of the offense . . . is [a]n intent to record a confidential communication.")); *People v. Buchanan*, 126 Cal. App. 3d 274, 289 (1972) (no intent where defendant overheard the conversation inadvertently rather than intentionally). Given Google's clear prohibitions against the transmission of health information, Plaintiffs cannot allege that Google willfully read or intentionally recorded that same information.

Section 631: Google functioned as an extension of the Websites, and as such, cannot be considered an "eavesdropper" under Section 631. The relevant law in this District is summarized in *Doe v. Kaiser Foundation Health Plan, Inc.*, 2024 WL 1589982, at *14–18 (N.D. Cal. April 11, 2024), where Judge Chen concluded, "the critical question is the extent the third parties were subject to Kaiser's control and ability to limit the use of dissemination of the medical data." Here, the use of Google source code is subject to the websites' control and ability to limit the transmission, and even the use, of any data sent to Google. *See* SAC ¶¶ 105, 135, 154. Plaintiffs cannot support a claim based upon their speculation that Google Analytics settings and controls do not work as disclosed to effectuate developers' privacy preferences. *See, e.g.*, SAC ¶¶ 159 (claiming Google Analytics 4 feature that "IP addresses are not logged or stored" is ineffective);

135 (claiming turning off data sharing settings is ineffective); 157 (same).

The SAC also does not support Plaintiffs' allegations that Google read and learned the "contents" of Plaintiffs' communications. Plaintiffs claim that the "contents" consisted of URLs "disclosing searches for medical professionals specific to a plaintiff's medical needs, communications about bill payments, scheduling appointments, and specific conditions." Opp. at 16. However, even assuming that information constitutes content (it does not, *see* Mot. at 19), Plaintiffs' allegations and exhibits do not support that any of their information in these categories was sent to Google. Mot. at 8–9. For instance, John Doe V claims that analytics code was present on a Tallahassee Memorial Healthcare ("TMH") page about hip replacement surgery, but he does not allege that he ever visited that URL, nor that he did so due to a health condition. SAC ¶¶ 54, 57. Even if John Doe V had visited that TMH page, however, his allegations cannot fairly be distinguished from those in *Cedars-Sinai*, where plaintiffs alleged that they searched for ankle surgery, podiatrists, ophthalmologists, booked appointments, viewed medical tests, and that Cedars-Sinai transmitted that information to third parties, including Google. *Doe v. Cedars-Sinai Health Sys.*, 2024 WL 3303516, at *2 (Cal. Super. June 5, 2024).[2] The court found that no "contents of a communication" were transmitted, because the allegations "do not state the contents of Plaintiffs 'personal search queries' or detailed 'descriptive URLs,'" but that only "IP addresses and the webpages were revealed." *Id.* at *3. And, even assuming content was inadvertently transmitted to Google, the facts alleged do not support that Google attempted to "read" or "learn" the contents of those communications, as Plaintiffs do not even claim that Google targeted them with ads or personalized content based on that information. *Supra* Section II.B.1.

Section 632: The SAC makes clear that the Websites, not Google, recorded the data transmitted. The allegations (and contradictions) on the face of the SAC make clear that websites choose whether and where to place the Google source code on their webpages (SAC ¶¶ 114, 154), what custom events to record (*id.* ¶¶ 86–87), and what optional features to enable or disable (*id.*

[2] Plaintiffs take issue with Google's citation to *Cedars-Sinai*, Opp. at 16 n.2, citing California Rule of Court 8.1115, but that rule applies to appellate opinions only, and in any event, the California Rules of Court do not apply to cases in the Northern District of California.

¶¶ 27, 105, 135, 159). In addition, any communications allegedly recorded were not "confidential." *Cedars-Sinai*, 2024 WL 3303516, at *4 ("The IP addresses, webpages, and doctors' names are not confidential communications."). Again, Plaintiffs' allegations here cannot be fairly distinguished from those in *Cedars-Sinai*, where the plaintiffs alleged they conducted searches on Cedars-Sinai's website for ankle surgery and podiatrists, communicated personal medical information, booked appointments, viewed medical tests, and searched for ophthalmologists. *Id.* at *4. The plaintiffs also alleged that Cedars-Sinai collected IP addresses, "the pages a patient clicked on, and doctors' names on those pages." *Id.* The court found that the data plaintiffs alleged was collected did not consist of confidential communications under Section 632. *Id.*

3. Plaintiffs fail to plead privacy claims (Counts 3 and 4).

First, intrusion upon seclusion is an intentional tort and failure to plausibly allege intent is fatal to the claim. *Taus v. Loftus*, 40 Cal. 4th 683, 725 (2007). Plaintiffs do not appear to dispute that their intent allegations are insufficient. Instead, they argue that intent is but "one of 'the surrounding circumstances' that determines whether an alleged intrusion is serious and highly offensive." Opp. at 18. But this Court has already dismissed Plaintiffs' privacy claims for failing to properly allege intent. Order at 13. And, Plaintiffs' own authorities work against them. *See, e.g.*, *Hernandez v. Hillsides, Inc*., 47 Cal. 4th 272, 294–96 (2009) ("no cause of action will lie for accidental, misguided, or excusable acts of overstepping upon legitimate privacy rights.").

Second, Plaintiffs do not—and cannot—allege that Google knew they were patients of the Websites. "Without knowing information that's never received—i.e., the visitor's subjective motive—the resulting metadata could never identify that individual's PHI." *Am. Hosp. Ass'n v. Becerra*, 2024 WL 3075865, at *13 (N.D. Tex. June 20, 2024). Plaintiffs attempt to brush aside *American Hospital Ass'n* as irrelevant. Opp. at 18–19. This misses the requirement that Plaintiffs' reasons for visiting the page, otherwise unknown to Google, be *communicated. Am. Hosp. Ass'n*, 2024 WL 3075865, at *15. Not only is there no allegation that the visitor's subjective motive was communicated to Google (e.g., whether they were visiting as a patient or researcher) but Plaintiffs' "sample" transmissions do not even contain the type of information HHS notes may disclose PHI.

See Dkt. Nos. 158-1, 158-2. For these reasons, the data transmitted to Google does not "capture[] information that connects a particular user to a particular healthcare provider." *See* Opp. at 19.

Third, Plaintiffs do not explain how the alleged intrusion occurred in a highly offensive manner. "Contemporary internet browsing involves the collection of users' data, including by tracking users across the internet, *and a reasonable user should expect as much*." *Hubbard v. Google LLC*, 2024 WL 3302066, at *2, *7–8 (N.D. Cal. July 1, 2024) (emphasis in original) (holding that the collection of "searches run, videos watched, views and interactions with content and ads, voice and audio information, purchase activity, people with whom a user communicated, browsing history," "activity on third-party sites and apps that used Google services," "GPS," "device sensor data," "data from devices located near a user," and "advertising ID" did not rise to the level of a highly offensive intrusion). Plaintiffs inexplicably conflate the term "Health Information" in Google's Privacy Policy, which is clearly defined as actual medical records or metrics about a specific person, with the information Plaintiffs actually allege Google collected and used. *See* Opp. at 19; Dkt. 158-14 at 19. Nor can Plaintiffs' distinguish their allegations of intent from the ones that Judge Chen held did not amount to a highly offensive intrusion in *Kaiser Foundation Health Plan, Inc.*, 2024 WL 1589982, at *19. *See* Opp. at 20. As was the case in *Kaiser,* Plaintiffs' allegations of Google's knowledge and intent are poorly pled. *See* Mot. at 12–14; *supra* Section II.C.

Finally, recognizing the gaps in the SAC, Plaintiffs claim that none of their claims "are based on receiving advertisements; . . . what is offensive is that Google does 'far more with the information than store it.'" Opp. at 19. But Plaintiffs never explain what exactly Google does *with sensitive health data*, if not personalize advertising, that invades user privacy. While Plaintiffs allege that data from the Websites "flows into Google's advertising systems," they do not competently allege that this is true for their sensitive health information. And how such alleged flow of data connects to an alleged use of health information in a highly offensive manner is completely unexplained.

4. Plaintiffs fail to identify a breach of Google's Privacy Policy (Count 5).

Promise 1: "Health Information" is defined in Google's Privacy Policy as "medical history, vital signs and health metrics (like blood glucose levels), and other similar information related to your physical or mental health, in the course of using Google services that offer health-related features, such as the Google Health Studies app." Dkt. 158-14 at 19. As this Court previously held, Plaintiffs do not allege that such information was collected. Order at 18. Instead, Plaintiffs again seek to re-write the Privacy Policy despite its clear language. Plaintiffs claim that a reasonable user would understand from the structure and the text of the Privacy Policy that its provision regarding "Health Information" applies to information other than the information Google says it applies to. Opp. at 21–22. Plaintiffs do not cite any authority to support their deviation from the plain language of the Privacy Policy. Neither *Calhoun v. Google LLC*, 2024 WL 3869446 (9th Cir. Aug. 20, 2024) nor *In re Meta Healthcare Pixel Litig.*, 647 F. Supp. 3d 778 (N.D. Cal. 2022) address the meaning to be given to a contractual term that is clearly defined in the contract. Opp. at 21.

Plaintiffs do not dispute that the Privacy Policy discloses that it collects Internet activity information, or that it identifies controls governing such collection. They argue, however, that the Court should disregard these provisions because the "specific" term governing Health Information prevails over the "general" terms about web activity. Opp. at 21. Plaintiffs omit that this canon of interpretation only applies when the terms conflict. *S. Cal. Gas Co. v. City of Santa Ana*, 336 F.3d 885, 892 (9th Cir. 2003). Plaintiffs do not identify a conflict, and *Smith v. Facebook, Inc.*, 745 F. App'x 8 (9th Cir. 2018) and *Kurowski v. Rush Sys. For Health*, 2024 WL 3455020 (N.D. Ill. July 18, 2024) show there is none. Mot. at 23. Plaintiffs cannot state a claim by ignoring the rest of the Privacy Policy. *See In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 832–33 (N.D. Cal. 2020) (dismissing claim that Google breached Privacy Policy by sharing data without consent where Plaintiffs failed to address other circumstances enabling Google to share data).

Promise 2: Plaintiffs claim Google breached a promise not to use health information for personalized advertising *not by showing personalized ads*, but by using their data in advertising products such as placement targeting, artificial intelligence, developing new services, and

personalized recommendations. Opp. at 22–23. This Court has already rejected Plaintiffs' recycled argument: "Google promised not to show personalized ads based on health, and the plaintiffs fail to allege they received any personalized ads based on their health." Order at 19. The portions of the Privacy Policy Plaintiffs rely on only relate to information used to *show* ads. *See* SAC ¶ 287; Dkt. 158-14. How these alleged uses pertain to *personalized* advertising is not explained.

In any event, Plaintiffs have not alleged that their health information was used for any of these purposes. The documents that Plaintiffs rely upon do not mention health information, but are simply disclosures and Help Pages that describe how Google's products work in general.

5. Plaintiffs fail to identify a breach of the implied covenant (Count 6).

In their Opposition, Plaintiffs argue that Google breached the implied covenant by "selectively interpreting" contractual terms (Opp. at 24)—terms that Plaintiffs also allege Google breached outright (SAC ¶¶ 285–87, 289–91). A breach of the implied covenant requires conduct that "injure[s] the rights of [a party] to receive the benefits of [the] agreement." *Careau & Co. v. Sec. Pac. Bus. Credit, Inc.*, 222 Cal. App. 3d 1371, 1393 (1990). But the SAC alleges no such conduct. It does not allege, for example, that Plaintiffs ever sought to assert a contractual right and that Google, in response, acted in bad faith to deny Plaintiffs the benefit of the bargain. *Cf. Perez-Encinas v. AmerUs Life Ins. Co.*, 468 F. Supp. 2d 1127, 1139 (N.D. Cal. 2006) (describing the "typical case" of breach of the implied covenant as "stonewalling by an insurance company so as to avoid its duty to make payments and thus reap some benefit for itself"). Plaintiffs' essential claim here is that Google breached the contract; the SAC does not adequately allege that Google did anything else to deny Plaintiffs the benefit of the bargain. *See Guz v. Bechtel Nat'l Inc.*, 24 Cal. 4th 317, 352–53 (2000) ("To the extent the implied covenant claim seeks simply to invoke terms to which the parties did agree, it is superfluous.").

The Opposition's *ipse dixit* that "Google's interpretations" of the contract "are unreasonable" does not make them so. And Plaintiffs do not even identify—in their SAC or Opposition—any "interpretations" by Google beyond those Google has offered in the context of this litigation, which cannot give rise to tort liability. *See Lopez Reyes v. Kenosian & Miele, LLP*,

525 F. Supp. 2d 1158, 1160–62 (N.D. Cal. 2007). The Opposition thrice asserts that "it is reasonable to read" the at-issue contractual terms as Plaintiffs do. Opp. at 24. Google disagrees. But the reasonableness of Plaintiffs' interpretations is irrelevant. Plaintiffs must at the very least allege "conduct" with respect to the contract that is "objectively unreasonable." *See Carma Devs. (Cal.), Inc. v. Marathon Dev. Cal., Inc.*, 2 Cal.4th 342, 372 (1992). In dismissing Plaintiffs' implied-covenant claim in the FAC, the Court correctly concluded that "[P]laintiffs have not adequately alleged that Google's interpretation of 'health information' or 'personally identifiable information' is objectively unreasonable." Order at 20. The implied-covenant claim in the SAC fails for the same reason.

6. Plaintiffs fail to state a claim for unjust enrichment (Count 7).

Plaintiffs' Opposition does not even try to grapple with *Saroya v. University of the Pacific*, 503 F. Supp. 3d 986, 998–99 (N.D. Cal. 2020), which explains that, although a "plaintiff may assert inconsistent theories of recovery at the pleading stage, . . . a plaintiff may not plead the existence of an enforceable contract and simultaneously maintain a quasi-contract claim unless the plaintiff also pleads facts suggesting that the contract may be unenforceable or invalid." Like the plaintiff in *Saroya*, Plaintiffs plead the existence of an enforceable contract but do *not* plead any facts suggesting that the contract may be unenforceable or invalid. Plaintiffs' unjust-enrichment claim thus founders on this point of substantive law. (The case of *Astiana v. Hain Celestial Group, Inc.*, 783 F.3d 753, 762 (9th Cir. 2015), which Plaintiffs rely on, is inapposite because it did not involve concurrent claims for unjust enrichment and breach of contract). Plaintiffs' bid to plead these incompatible claims "in the alternative" founders on procedural law as well: "Rule 8(d)(2) requires that 'alternative statements' be 'set out' in the pleading, a requirement that is generally met through 'either-or propositions' or 'if-then allegations.'" *Sun Life Assurance Co. of Can. v. Imperial Premium Fin., LLC*, 904 F.3d 1197, 1213 n.16 (11th Cir. 2018) (citations omitted). The SAC sets out no such alternative statements.

III. CONCLUSION

Google respectfully requests that the Court dismiss the SAC with prejudice.

Dated: September 24, 2024

WILLKIE FARR & GALLAGHER LLP
Benedict Hur
Simona Agnolucci
Eduardo Santacana
David Doak
Joshua Anderson
Tiffany Lin
Harris Mateen
Naiara Toker
Nadim Houssain

By: */s/ Benedict Hur*
Benedict Hur

Attorneys for Defendant
GOOGLE LLC